4T-06

# コンソーシアムブロックチェーンを用いた DNS 権威サーバの分散管理の提案

服部　氷河 [†1]　加藤 宏理 [†2]　鈴木　洸太 [†2]　鈴木　秀和 [†2]
[†1] 名城大学理工学部　[†2] 名城大学大学院理工学研究科

## 1　はじめに

インターネットサービスの可用性を維持するために，DNS サーバに対する DDoS 攻撃の対策を行うことは重要である．現在の DNS 多重化では DNS 権威サーバを複数台用意し，マスターサーバからスレーブサーバにゾーンデータを転送することで分散管理を行い，障害耐性を確保している [1]．そのため，高い可用性の実現にはサーバを増やす必要があり，運用コストが増加する．

本稿では，一定数の DNS 権威サーバを一つのグループと定義し，DNS レコードをブロックチェーンを用いて分散管理する手法を提案する．従来の DNS におけるマスターサーバとスレーブサーバで多重化するのではなく，グループ内の全権威サーバが DNS レコードの情報を分散台帳で管理する．これにより，特定の権威サーバに DDoS 攻撃が行われ障害が発生しても別サーバで名前解決できるアーキテクチャを実現する．

## 2　提案手法

### 2.1　概要

本稿では，コンソーシアムブロックチェーンを用いて権威サーバ同士でデータを共有する．共有したデータをもとにそれぞれの権威サーバが他の権威サーバのスレーブサーバとしての役割も持つ新たな DNS を提案する．これにより，低コストで DDoS 攻撃に強い DNS を実現する．

### 2.2　提案手法における分散管理の方法

提案手法では一定数の DNS 権威サーバでグループを形成し，同じグループ内の DNS 権威サーバでブロックチェーンを構成する．このブロックチェーンを利用し，図 1 のようにゾーンデータをグループ内の他の権威サーバへコピーすることで分散管理を行う．

ブロックチェーンを構成している DNS ドメイン階層

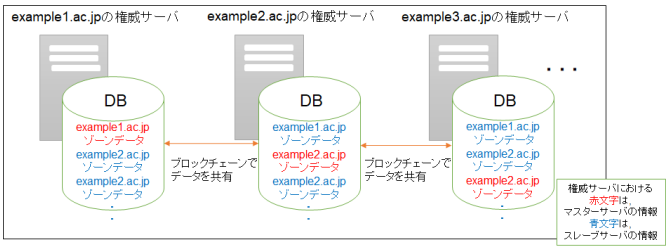


図 1　提案手法における分散管理の方法

表 1　グループ情報

| 管理項目 | 概要 |
|---|---|
| グループ ID | グループを識別する ID |
| ドメイン名 | ドメイン名 |
| IP アドレス | 問い合わせ先権威サーバの IP アドレス |
| 状態フラグ | サーバ状態を示すフラグ (RUNNING/DOWN) |

表 2　代替権威サーバの IP アドレス情報

| 管理項目 | 概要 |
|---|---|
| ドメイン名 | 問い合わせたいドメイン名 |
| 代替 IP アドレス | 代替となった問い合わせ先権威サーバの IP アドレス |

よりも 1 つ上の階層の権威サーバにて，下位の権威サーバがダウンした際に振り分けを行うためのグループ情報を表 1 のように管理する．

### 2.3　サーバダウン判定時の動作

目的の権威サーバに対し IP アドレスの問い合わせを行ったとき，一定時間内に返答が行われなければその権威サーバはサーバがダウンしていると判定する．

サーバがダウンしていると判定された場合は，グループ情報テーブル内の状態フラグを DOWN に変更し，グループ ID が同じ権威サーバの中から代替の権威サーバをランダムに選択する．ランダムに選択された権威サーバの IP アドレスを表 2 に示す代替権威サーバの IP アドレス情報テーブルにドメイン名とともに格納する．

### 2.4　提案手法における名前解決の動作

#### 2.4.1　状態フラグが RUNNING の場合の動作

1. グループ情報から問い合わせ先権威サーバの IP アドレスを検索し，その IP アドレスへ問い合わせを行う．
2. 権威サーバは問い合わせの結果を返す．

**A Proposal for Distributed Management of DNS Authoritative Servers Using Consortium Blockchain**

Hyoga Hattori[†1], Hirotoshi Kato[†2], Kota Suzuki[†2], and Hidekazu Suzuki[†2]
[†1] Faculty of Science and Technology, Meijo University
[†2] Graduate School of Science and Technology, Meijo University

#### 2.4.2 状態フラグが DOWN の場合の動作

1. 代替権威サーバの IP アドレス情報から代替となった権威サーバの IP アドレスを検索し，その IP アドレスへ問い合わせを行う．
2. 代替となった権威サーバは，どこのドメインの IP アドレスを問い合わせしているかを確認し，ブロックチェーンで共有しているデータの中から目的のドメインの IP アドレスを返す．

### 2.5 サーバ再起動時の動作

ダウンしていたサーバが復旧した際には，グループ情報テーブルにて管理している他の権威サーバに対して，サーバ起動通知を行う．グループ情報テーブルを管理している権威サーバは，再起動した権威サーバのグループ情報テーブル内の状態フラグを RUNNING に変更し，代替権威サーバの IP アドレス情報からデータを削除する．

## 3 評価

### 3.1 定量的評価

提案手法を実装した DNS 権威サーバにおける各種処理時間の影響を検証するために，AWS EC2 の t2.micro 上に MariaDB をインストールをし，問い合わせ先となる権威サーバの IP アドレスを検索するまでの時間及び代替権威サーバの選択処理時間を評価した．

今回の検証では，文献 [2] で示されている co.jp のドメイン名数を参考に，46 万件のデータを 1,000 個のグループに分けてグループ情報テーブルに登録した．このうち，ダウンしているサーバを 1,000 件選択した．この条件にて，問い合わせ先権威サーバの IP アドレスを取得するまでの時間および代替権威サーバの IP アドレス選択に要した処理時間を計測した．

表 3 に権威サーバの IP アドレス検索時間の結果を示す．提案手法は従来手法に比べ，1 回の名前解決処理あたり最大で 206ms の処理時間が増加することが分かった．表 4 に代替権威サーバの検索処理時間の結果を示す．権威サーバがダウンしている場合，最大で 242ms の処理時間が必要となることが分かった．一般的に DNS の名前解決処理のタイムアウトが秒単位で設定される場合が多いため，提案手法に伴うオーバヘッドが発生しても，リトライなしで通常または代替の権威サーバへ問い合わせを行うことは可能であることを確認できた．

### 3.2 定性的評価

表 5 に従来手法と提案手法の比較を示す．従来手法と提案手法の処理時間を比較すると，一度の名前解決にかかる時間が最大 206ms 増加する結果になった．文献 [3] によると DNS サービスの平均応答時間は 68.23ms となっている．そのため，206ms の結果は平均応答時間から見ても大幅な上昇となる．したがって，高速な処理が可能である DB に変えるなどの検討が必要である．代替の権威サーバの IP アドレスを選択するのに要する時間は最大 242ms となったが，この処理はサーバダウン時のみ実行されるため，サーバダウンが多発しなければ実用上問題ないと考えられる．

表 3　問い合わせ先権威サーバの IP アドレス検索時間

| | 最小 [ms] | 平均 [ms] | 最大 [ms] |
|---|---|---|---|
| サーバ正常動作時 | 200 | 203 | 205 |
| サーバダウン時 | 200 | 204 | 206 |

表 4　代替権威サーバの IP アドレス選択時間

| | 最小 [ms] | 平均 [ms] | 最大 [ms] |
|---|---|---|---|
| 処理時間 | 236 | 239 | 242 |

表 5　従来手法と提案手法の比較

| | 従来手法 | 提案手法 |
|---|---|---|
| 処理時間 | ○ | △ |
| コスト | × | ○ |

従来手法では，マスターとなる権威サーバ 1 台につき，スレーブサーバを最低 1 台構築しないと障害耐性を保つことができない．大規模なシステムであれば，スレーブサーバを複数台構築するケースもある．提案手法では組織当たりで構築および管理する権威サーバはマスター 1 台でよく，スレーブサーバが不要となる．したがって，スレーブサーバの台数分の導入および運用コストを削減することができる．また，グループ内のすべてのサーバをスレーブサーバとして使うことが可能なため，従来手法よりも安定した DNS の運用が可能であると考えられる．以上より，低コストで障害耐性のある DNS 運用が可能である．

## 4 まとめ

本稿では，低コストで障害耐性のある DNS のアーキテクチャを提案した．また，従来手法より処理が増えることによるスループットを検証した．

#### 参考文献

[1] P. Hoffman, *et al.*: RFC 8499, IETF (2019). https://tools.ietf.org/html/rfc8499
[2] 株式会社日本レジストリサービス (2021). https://jprs.jp/about/stats/
[3] Cloudflare DNS https://1.1.1.1/ja-jp/